



STORMSHIELD



GUIDE

**STORMSHIELD DATA SECURITY
ENTERPRISE**

ADVANCED CONFIGURATION GUIDE

Version 11.4

Document last updated: July 22, 2025

Reference: sds-en-sdse-advanced_configuration_guide-v11.4



Table of contents

1. Getting started	4
2. Configuring a security policy in a .json file	5
2.1 Account	5
2.1.1 parameters	5
2.1.2 creation	9
2.1.3 recovery	12
2.1.4 keyRing	12
2.1.5 renewal	13
2.2 Policy certificates	13
2.3 Policy directories	14
2.4 Stormshield Data File	16
2.4.1 decryptionList section	18
2.4.2 encryptionList section	19
2.4.3 exclusionList section	21
2.5 Stormshield Data Team	22
2.6 Stormshield Data Disk	25
2.7 Stormshield Data Mail	27
2.8 Stormshield Data Sign	29
2.9 Stormshield Data Shredder	30
2.9.1 exclusionList section	31
2.9.2 shreddingList section	32
2.10 Stormshield Data Share	34
2.11 Directories	35
2.11.1 ldap section	35
2.11.2 pgp section	38
2.12 Certificate revocation	38
2.13 Distribution points	39
3. Configuring advanced parameters in the registry base	41
3.1 Team Feature	41
3.1.1 Changing the dates of the last access	41
3.1.2 Check user key certificate	41
3.2 Manage encryption and signature keys	42
3.2.1 Specify that keys are generated by SDS Enterprise	42
3.2.2 Choose how to keep keys for exporting later	42
3.3 Moving folders available offline	43
3.4 Keeping performance optimal on the workstation	43
3.4.1 Improving performance when browsing encrypted trees	43
3.4.2 Excluding Windows processes that access encrypted folders	43
3.4.3 Excluding Windows Defender extensions and scans	44
3.5 Disabling automatic suggestion of coworkers	44
3.6 Configure the filter for the coworker search in the LDAP directory	44
3.7 Show license key value	45
3.8 Manage card or token readers	45
3.8.1 Specify card or token reader	45
3.8.2 Filter card or token readers by their description	46
3.8.3 Filter card or token readers by manufacturer ID	46
3.8.4 Prohibit modification of card or token type	46
3.9 Replace default icon for Share-protected collaborative folders	46



4. Further reading48

In the documentation, Stormshield Data Security Enterprise is referred to in its short form: SDS Enterprise and Stormshield Data Management Center in its short form: SDMC.



1. Getting started

This guide describes the use of configuration files and the Windows registry base to configure SDS Enterprise security policies.

Stormshield Data Security Enterprise policy parameters can be configured in several ways:

- In the **SDMC administration console**, which can be accessed at <https://sds.stormshieldcs.eu/admin>. The console allows you to create and configure security policies via a graphical interface that feeds the *.json* configuration file. For more information, refer to the *Managing security policies in SDMC* in the Administration guide. A number of advanced parameters are not available in SDMC, but only in the different configuration files below.
- Directly in ***.json* configuration files** that contain the large majority of the configuration parameters found in security policies. There is one file per security policy. For more information, refer to the section [Configuring a security policy in a .json file](#). All parameters in the SDMC administration console can also be configured in the *.json* file.
- In the Windows registry base. For further information, refer to the section [Configuring advanced parameters in the registry base](#).



2. Configuring a security policy in a .json file

1. Create and configure a security policy in the SDMC administration console. This generates a file in JSON format with the name of the security policy, for example *defaultpolicy.json*. For more information, see section *Managing security policies in SDMC* in the Administration guide.
2. Download the file.
For more information, see section *Installing SDS Enterprise agents on user workstations* in the Administration guide.
3. Edit the .json file and manually modify its parameters. The file is divided into several sections, each of which correspond to a feature in SDS Enterprise. Various parameters are found in these sections.
The tables below contain the descriptions of the parameters, categorized by feature. Unless otherwise indicated, there must be parameters in the file. The tables also mention whether the parameter exists in the SDMC administration console and where to find it.

2.1 Account

User accounts are configured in the *accountPolicy* section of the .json file, itself divided into several subsections: *parameters*, *creation*, *recovery*, *keyRing* and *renewal*.

2.1.1 parameters

The operating parameters of user accounts can be configured in the *parameters* section described in the table below. In the SDMC administration console, the equivalent parameters are found in **Policies > Accounts > Parameters**.

For further information, refer to the section *Configuring generic account settings* in the Administration guide.

Parameter	Description	Possible values	SDMC
cryptography	Indicates how cryptographic operations are performed when the account is in use. This parameter impacts all functions of SDS Enterprise, except Data Disk .		Encryption and signature
	encryptionAlgorithm: Algorithm to use in encryption operations.	AES-256	Encryption algorithm
	hashAlgorithm: Algorithm to use in signature operations.	SHA-256, SHA-512	Signature algorithm
	keyEncryptionMethod: Optional. Algorithm to use in operations encrypting the keys. Allowed values are: <ul style="list-style-type: none">• "RSA-OAEP-SHA-256", default value,• "RSA-OAEP-SHA-1", compatibility value for old cards	RSA-OAEP-SHA-256, RSA-OAEP-SHA-1	N/A



Parameter	Description	Possible values	SDMC
primaryUserPath	<p>Optional. Tells the agent the primary path to use to retrieve application user accounts and create new users.</p> <p>The behavior differs for the two use cases:</p> <ul style="list-style-type: none">Account recovery: If this path is missing or invalid, the agent uses the secondaryUserPath.Account creation: If this path is missing, the agent uses the application's default path: <code><COMMON_APPDATA>\Arkoon\Security BOX\Users</code>. If it is invalid, the action fails.		
secondaryUserPath	<p>Optional. Tells the agent the secondary path to use if the primaryUserPath is absent or invalid.</p> <p>The behavior differs for the two use cases:</p> <ul style="list-style-type: none">Account recovery: If the secondaryUserPath is missing, the agent uses the <code><COMMON_APPDATA>\Arkoon\Security BOX\Users</code> path. If it is invalid, or if primaryUserPath was invalid, the action fails.Account creation: If the secondaryUserPath is missing, the agent uses the default path of the application: <code><COMMON_APPDATA>\Arkoon\Security BOX\Users</code>. If this path is invalid, the action fails.		
cardAccount	<p>Optional. Indicates how smart card accounts operate. This field appears only if the policy allows connections to smart card accounts.</p>		Card or USB token accounts



Parameter	Description	Possible values	SDMC
unfreezeOnCardInsertion	Optional. Specifies whether the session unlock window opens automatically when a card is inserted into the workstation. Allowed values are: <ul style="list-style-type: none">• “true” to open the window (default value),• “false” to not open the window.	true, false	N/A
connectOnCardInsert	Optional. Specifies whether the login window opens automatically when a card is inserted into the workstation. Allowed values are: <ul style="list-style-type: none">• “true” to open the window,• “false” to not open the window (default value).	true, false	N/A
enableRepairCardAccount	Optional. Makes it possible to repair a smart card if only the certificate is available, by renewing the key based on the known CKA_ID in the account. Allowed values are: <ul style="list-style-type: none">• “true” to enable repair,• “false” to disable repair (default value).	true, false	N/A
enableAutomaticRenewFromCard	Optional. When a user's new encryption or signature key is already in the card, this option automatically renews the key when the previous one expires. Allowed values are: <ul style="list-style-type: none">• “forbidden” to prohibit automatic renewal (default value),• “confirm” to automatically renew after confirmation by the user. After a refusal, renewal is no longer offered. Therefore, using this value is not recommended.• “silent” to automatically renew without user confirmation. In SSO mode, this value is forced even if another value is set.	forbidden, confirm, silent	N/A



Parameter	Description	Possible values	SDMC
cardMiddlewares	List of middleware programs that can be used on the workstation. Middleware allows SDS Enterprise to communicate with all types of smart cards and USB tokens. The Stormshield Smartcard Support middleware is included by default.		Middleware
	name: Name displayed for this middleware configuration.	String	
	dllname: Name of the DLL containing the middleware. The value is an absolute path to the DLL on the user's workstation. If the DLL is in a folder of the Windows PATH variable, the DLL name will suffice.	String	
	disablePKCS11Label, disablePKCS11Extractable, disablePKCS11Modifiable et disablePKCS11ModulusBits: Parameters that monitor the use of various PKCS#11 attributes during communication with smart cards/USB tokens. These parameters come from the database of known middleware programs on SDMC, and are entered to increase the agent's compatibility with middleware from various vendors. You are advised against modifying the default values provided.	true, false	
	showAllSlots: Indicates whether the "Information" window in the smart card configurator displays information about all logical slots managed by the middleware (true), or only slots with a smart card/token inserted (false).	true, false	



Parameter	Description	Possible values	SDMC
accountMode	<p>Indicates the user account types that can be connected. Allowed values are:</p> <ul style="list-style-type: none">• "password" for the <i>password</i> mode. Keys are stored in the keystore.usr file and protected by a password.• "smartcard" for <i>smart card</i> mode. Keys are stored on a smart card or USB token and protected by a PIN.• "SSO" for <i>single sign-on</i> mode, in which the account's keys are issued by the Windows keystore. This mode does not require authentication.• "passwordAndSmartcard" for <i>password</i> and <i>smart card</i> modes.	password, smartcard, SSO, passwordAndSmartcard	Account type

2.1.2 creation

The creation parameters of user accounts can be configured in the *creation* section described in the table below. In the SDMC administration console, the equivalent parameters are found in **Policies > Accounts > Creation**.

For further information, refer to the section *Setting account creation parameters* in the Advanced configuration guide.

Parameter	Description	Possible values	SDMC
accountKeyMode	<p>Indicates the operating mode of accounts when they are created. This parameter does not affect how existing accounts function. Allowed values are:</p> <ul style="list-style-type: none">• "singleKeyEncryption" for accounts with a single encryption key,• "singleKeySignature" for accounts with a single signature key,• "dualKey" for accounts with an encryption key and a signature key.	singleKeyEncryption, singleKeySignature, dualKey	Key management



Parameter	Description	Possible values	SDMC
passwordAccountMethod	Indicates whether password accounts can be created, and how. Allowed values are: <ul style="list-style-type: none">"forbidden" to prohibit the creation of password accounts,"manual" to allow users to create accounts manually.	forbidden, manual	General settings Password accounts
cardAccountMethod	Indicates whether smart card or USB token accounts can be created, and how. Allowed values are: <ul style="list-style-type: none">"forbidden" to prohibit the creation of smart card or token accounts,"manual" to allow users to create accounts manually,"automatic" to enable launching the creation of automatic accounts,"manualAndAutomatic" to combine the creation of manual and automatic accounts.	forbidden, manual, automatic, manualAndAutomatic	General settings Accounts Card or USB token
passwordAccount	Optional. Indicates password creation settings. This field does not appear if password account creation is prohibited.		Password account creation
passwordStrength	Indicating the strength of the password chosen by the user for the new account.		Password strength
	alphabeticCharMinCount: Minimum number of alphabetic characters that the user's password must contain.	Positive integer.	Minimum number of alphabetic characters
	numericCharMinCount: Minimum number of digital characters that the user's password must contain.	Positive integer.	Minimum number of numeric characters
	specialCharMinCount: Minimum number of special characters that the user's password must contain.	Positive integer.	Minimum number of special characters
	totalCharMinCount: Minimum number of characters that the user's password must contain.	Positive integer.	Minimum number of characters



Parameter	Description	Possible values	SDMC
	<p>allowedKeySources: List of sources from which users can choose keys for their accounts. Allowed values are:</p> <ul style="list-style-type: none">• "p12File" so that users will select a P12 file in which the keys to their account are saved,• "selfSignedP12" so that the user can ask SDS Enterprise to generate self-certified keys for their account.	p12File, selfSignedP12	Import .p12 certificates Generate .p12 certificates locally
	selfSignedOptions: Optional. Specific parameters relating to the generation of self-certified keys. This field does not appear if the manual creation of password accounts does not allow the use of self-certified keys.		Self-certified certificates
	baseLifetimeYears: Certificate validity in number of years from their creation date.	Positive integer.	Validity period of self-certified certificates issued by SDS upon account creation
	renewalPeriodYears: Certificate validity in number of years from their renewal date.	Positive integer.	Validity period of self-certified certificates issued by SDS upon key renewal
	keyType: Size of keys generated by SDS Enterprise when the account is created.	RSA-2048, RSA-4096	Key size
automatic	Optional. Settings relating to the automatic creation of accounts. This field may not appear if automatic account creation is prohibited.		Filter CAs on automatic creation
	encryptionKeyAuthorityId: Optional. Unique identifier of the authority providing the encryption keys to be used to create the account. You will find the ID in the list of authorities in the certificateData section of the <i>.json</i> file.	Unique character string	Authority name for decryption



Parameter	Description	Possible values	SDMC
	signatureKeyAuthorityId: Optional. Unique ID of the authority that issued the signature key to be used for creating the account. You will find the ID in the list of authorities in the certificateData section of the <i>.json</i> file.	Unique character string	Authority name for signature
allowedKeyTypesForP12Import	Optional. Used to define the type and size of keys authorized, along with the default value proposed when a user creates an account by importing a P12 file.		N/A
	type: type of key authorized for creation with a P12 file. A key type missing from the list is not proposed to the user. If the list is empty or the parameter is missing, the default key type proposed is RSA-4096.	RSA-2048, RSA-4096	N/A
	default: defines whether this key type is selected by default in the drop-down list proposed to the user in the window. If several key types have their default value set to true, RSA-4096 will be proposed by default.	true, false	N/A

2.1.3 recovery

The recovery parameters of user accounts can be configured in the *recovery* section described in the table below. In the SDMC administration console, the equivalent parameters are found in **Policies > Accounts > Data recovery**.

For more information, see the section *Enabling data recovery* in the Administration Guide.

Parameter	Description	Possible values	SDMC
certificateId	Unique ID of the recovery certificate to be added to users for the SDS Enterprise agent's encryption operations. You will find the identifier in the list of certificates in the certificateData section of the <i>.json</i> file.	Unique character string	Key management

2.1.4 keyRing

User key management parameters are configured in the *keyRing* section described in the table below. In the SDMC administration console, the equivalent parameters are found in the **Policies > Accounts > Keyrings** panel.

For more information, see *Managing the Keyring* in the Administration Guide.



Parameter	Description	Possible values	SDMC
encryptionKey	Optional. showTab: Shows or hides the Encryption tab in the user's keyring. The tab is displayed by default.	true, false	Encryption key
signatureKey	Optional. showTab: Shows or hides the Signature tab in the user's keyring. The tab is displayed by default.	true, false	Signature key
dualUseKey	Optional. showTab: Shows or hides the Personal key tab in the user's keyring. The tab is displayed by default.	true, false	Personal key
decryptionKey	Optional. showTab: Shows or hides the Decryption tab in the user's keyring. The tab is displayed by default.	true, false	Decryption key
recoveryKey	Optional. showTab: Shows or hides the Recovery tab in the user's keyring. The tab is displayed by default.	true, false	Recovery key

2.1.5 renewal

User key renewal parameters are configured in the *renewal* section described in the table below.

Parameter	Description	Possible values	SDMC
allowedKeyTypes	Optional. Defines the type and size of keys allowed when a user renews a key by generating a new one.		
	type: type of key allowed for renewal. A key type missing from the list is not proposed to the user. If the list is empty or if the parameter is missing, the default key type proposed in the renewal window is RSA-4096.	RSA-2048, RSA-4096	N/A
	default: defines the default key type selected from the drop-down list offered to the user in the renewal window.	true, false	N/A

2.2 Policy certificates

The list of certificates used in the policy is specified in the *certificateData* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Certificate library**.

For more information on certificates, refer to the section *Managing authority certificates and recovery certificates in SDMC* in the Administration guide.



Parameter	Description	Prescribed values	SDMC
certificateData	List of certificates used in the policy.		
	id : Unique ID of the certificate in the policy. Used in other sections of the <i>.json</i> file to identify the certificate. See the example below.	Unique character string.	N/A
	data: Value of the certificate encoded in Base64.	Character string	N/A

Example of a list of two certificates. The first represents the certificate of the authority that issues the keys to be used for creating an automatic account.

```
"certificateData": [  
  {  
    "id": "0123456789ab-cdef-0123-4567-89abcdef",  
    "data": "LS0tLS1CRUdJTiBDRVJU..."  
  },  
  {  
    "id": "fedcba987654-3210-fedc-ba98-76543210",  
    "data": "U1EWURDQ0FraWdBd0lCQ..."  
  },  
]
```

The ID of the first certificate "0123456789ab-cdef-0123-4567-89abcdef" is therefore used as the value in the parameters `encryptionKeyAuthorityId` and `signatureKeyAuthorityId` in the automatic account creation policy (`accountPolicy` section):

```
"automatic": {  
  "encryptionKeyAuthorityId": "0123456789ab-cdef-0123-4567-  
89abcdef",  
  "signatureKeyAuthorityId": "0123456789ab-cdef-0123-4567-89abcdef"  
}
```

2.3 Policy directories

The list of LDAP directories used in the policy is specified in the *ldapData* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in the **LDAP library** panel.

For more information on certificates, refer to the section *Managing LDAP directories in SDMC* in the Administration guide.

Parameter	Description	Prescribed values	SDMC
id	Unique ID of the LDAP directory in the policy. Used in other sections of the <i>.json</i> file to identify the directory.	Unique character string.	N/A
configuration	LDAP directory configuration		
name	Configuration name.	Character string	Server name



Parameter	Description	Prescribed values	SDMC
access	LDAP server contact settings.		N/A
	address: Server address.	Character string	Address
	port: Port to use.	Integer between 0 and 65536	Connection port
	protocol: Protocol to use. Allowed values are: <ul style="list-style-type: none"> "ldap" for the standard LDAP protocol, "ldaps" for the secure LDAP protocol, "ldapsWithFallbackToLdap" to attempt an LDAP connection if the LDAPS connection fails. 	ldap ldaps, ldapsWithFallbackToLdap	Use an LDAPS connection Try to connect with LDAP if LAPS connection fails
credentials	Connection ID.		Access control
	username: User name. The "<Myself>" value makes it possible to use the Windows session identifiers.	Character string	ID
	password: Password. The "<Myself>" value makes it possible to use the Windows session identifiers.	Character string	Password
advanced	Search settings.		Search
	base: Base of an LDAP request.	Character string	Base
	depth: Search depth. Allowed values are: <ul style="list-style-type: none"> "minimum" to perform the search on the immediate level in the tree, "oneLevel" to perform the search on the immediate level and on a lower level only, "maximum" to perform the search recursively in the tree. 	minimum, oneLevel, maximum	Depth
	timeoutSeconds: Timeout of the request before canceling (in seconds).	Positive integer >= 10	Timeout before canceling connection request (in seconds)
searchAttributeNames	Names to use to request various attributes during the search.		Search attribute names
	emailAddress: Name of the attribute containing the e-mail address. The default value is "mail".	Character string	E-mail address



Parameter	Description	Prescribed values	SDMC
	commonName: Name of the attribute containing the common name. The default value is "cn".	Character string	Common name
	certificate: Name of the attribute containing the certificate. The value by default is "usercertificate;binary".	Character string	Certificate

2.4 Stormshield Data File

Stormshield Data File can be configured in the *filePolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > File**.

For more information on configuring this feature, refer to the section *Configuring Stormshield Data File* in the Administration guide.

Parameter	Description	Possible values	SDMC
fileFormat	Format of the encrypted file.	sdsx, sbbox	Encryption format
forceTranscipheringToSdsx	Optional. Only when <i>.sdsx</i> format is chosen for the "fileFormat" parameter: automatically converts <i>.sbbox</i> files to <i>.sdsx</i> format when the user opens them. By default, the value is "false".	true, false	Force conversion of <i>.sbbox</i> files to <i>.sdsx</i> format
moveTranscipheredSbox	Technical parameter required to operate the <i>moveTranscipheredSboxTo</i> parameter below. Its value is not taken into account by the SDS Enterprise agent.	true, false	
moveTranscipheredSboxTo	Specifies where to move <i>.sbbox</i> files upon conversion if the "forceTranscipheringToSdsx" parameter is enabled. If this setting is empty or missing from the policy, or if the designated path is inaccessible during conversion, the <i>.sbbox</i> file remains in its original location, next to the new <i>.sdsx</i> file.	String	After conversion, move the <i>.sbbox</i> files to
allowFileEncryption	Indicates whether the user is allowed to encrypt files.	true, false	Enable file encryption
allowNetworkEncryption	Indicates whether the user is allowed to encrypt network files.	true, false	Enable network file encryption
allowNetworkDecryption	Indicates whether the user is allowed to decrypt network files.	true, false	Enable network file decryption



Parameter	Description	Possible values	SDMC
allowFileDecryption	Indicates whether the user is allowed to decrypt files.	true, false	Enable file decryption
allowFolderEncryption	Indicates whether the user is allowed to encrypt folders.	true, false	Enable folder encryption
allowFolderDecryption	Indicates whether the user is allowed to decrypt folders.	true, false	Enable folder decryption
confirmForEachFile	If several files are being encrypted, indicates whether a confirmation is required for each file.	true, false	Confirm encryption for each file
allowEncryptionForRecipient	Indicates whether the user is allowed to encrypt files for themselves or for a recipient.	true, false	Enable file encryption for a recipient
allowSelfDecryptableFilesCreation	Indicates whether the user is allowed to create self-decryptable files.	true, false	Enable creation of self-decryptable files
allowEncryptSmartFile	Indicates whether the user is allowed to create smartFILE files.	true, false	Allow creation of smartFILE files
readOnlyFilesEncryption	Indicates how to process read-only files.	treatAsUsual, askConfirmation, doNotEncryptButNotify, neitherEncryptNorNotify	Process normally like standard files, Request confirmation, Notify but do not encrypt, Neither notify nor encrypt
autoEncryptDecryptedFolder	Enables or disables automatic Windows encryption on the temporary directory for decrypting .sdsx files (directory C:\Users\[user]\AppData\LocalLow\Stormshield\Stormshield Data Security\Decrypted).	true, false	Windows encryption of the decryption temporary directory
exclusionList	Specifies the parameters of the exclusion list. To use this list, refer to exclusionList section .	Exclude list	exclusionList



Parameter	Description	Possible values	SDMC
decryptionList	Specifies the parameters of the automatic file decryption list. To use this list, refer to decryptionList section .	Decryption list	decryptionList
encryptionList	Specifies the parameters of the automatic file encryption list. To use this list, refer to encryptionList section .	Encryption list	encryptionList
allowTranscipheringWithDelegationKeys	Optional. Specifies whether decryption with delegation keys is allowed. By default, the value is "false".	true, false	N/A
encryptHiddenFiles	Indicates whether hidden files must be encrypted.	true, false	Encrypt hidden files
blockedExtensionsOnOpening	Types of files that must first be decrypted before opening.	List of extensions in .ext format	N/A

2.4.1 decryptionList section

Files included in decryption lists are automatically decrypted at a predetermined time or when a predetermined event takes place. The following parameters are specified in the *filePolicy.decryptionList* section of the *.json* file.

Parameter	Description	Possible values	SDMC
askConfirmation	Indicates whether a confirmation is required before automatic decryption.	true, false	Ask confirmation before performing automatic decryption
displayReport	Indicates whether to display a report after automatic decryption.	true, false	Display report after performing automatic decryption
files	List of files to decrypt automatically.		Files decrypted automatically
	path: File path. To indicate several files, the "files" list must contain several objects, each with a different "path" property. For example: <pre>"files": [{ "path": "path1" }, { "path": "path2" }]</pre>	String	File path
folders	List of folders to decrypt automatically.		



Parameter	Description	Possible values	SDMC
	path: Folder path. To indicate several folders, this parameter must be used several times. See the "files" parameter.	String	Folder path or mask
	recursive: Indicates whether sub-folders are included in the decryption list.	true, false	Include sub-folders
masks	List of masks to decrypt automatically. To indicate several masks, this parameter must be used several times. See the "files" parameter.		
	path: Mask path. To indicate several masks, this parameter must be used several times. See the "files" parameter.	String	Folder path or mask
	recursive: Indicates whether sub-folders are included in the decryption list.	true, false	Include sub-folders
onConnection	Decrypts the list of files upon connection to SDS Enterprise.	true, false	Decrypts automatically upon connection to the SDS Enterprise account
onScreenSaverOver	Decrypts the list of files when screensaver stops.	true, false	Decrypt automatically when screensaver stops
onSessionUnlock	Decrypt the list of files when unlocking session.	true, false	Decrypt automatically when unlocking session

2.4.2 encryptionList section

Files included in encryption lists are automatically encrypted at a predetermined time or when a predetermined event takes place. The following parameters are specified in the *filePolicy.encryptionList* section of the *.json* file.

Parameter	Description	Possible values	SDMC
askConfirmation	Indicates whether a confirmation is required before automatic encryption.	true, false	Ask confirmation before performing automatic encryption
displayReport	Indicates whether to display a report after automatic encryption.	true, false	Display report after performing automatic encryption
files	List of files to encrypt automatically.		Files encrypted automatically



Parameter	Description	Possible values	SDMC
	<p>path: File path. To indicate several files, the "files" list must contain several objects, each with a different "path" property. For example:</p> <pre>"files": [{ "path": "path1" }, { "path": "path2" }]</pre>	String	File path
fixedTimesInSeconds	List of times at which files are automatically encrypted. Expressed in number of seconds from 00:00. For example, 1:30 a.m. is represented by a value of 5400.	List of positive whole integers	N/A
folders	List of folders to encrypt automatically.		
	path: Folder path. To indicate several folders, this parameter must be used several times. See the "files" parameter.	String	Folder path
	recursive: Indicates whether sub-folders are included in the encryption list.	true, false	Include sub-folders
intervalMinutes	Frequency with which files are automatically encrypted. Expressed in minutes.	Positive integer.	Automatic encryption frequency
masks	List of masks to encrypt automatically.		
	path: Mask path. To indicate several masks, this parameter must be used several times. See the "files" parameter.	String	Folder path or mask
	recursive: Indicates whether sub-folders are included in the encryption list.	true, false	Include sub-folders
onDisconnection	Enables list when disconnecting from SDS Enterprise.	true, false	Encrypt automatically when disconnecting from the SDS Enterprise account
onScreenSaverStarted	Enables the list when screensaver starts.	true, false	Encrypt automatically when screensaver starts
onSessionLock	Enables the list when locking the SDS Enterprise session.	true, false	Decrypt automatically when locking session



2.4.3 exclusionList section

Using an exclusion list, you can exclude some files to prevent them from being encrypted by mistake. The following parameters are specified in the *filePolicy.exclusionList* section of the *.json* file.

Parameter	Description	Possible values	SDMC
displayWarning	Indicates whether a warning window must be displayed if an operation could not be completed because of the exclusion list.	true, false	Display warning when encryption is rejected
files	List of files to be excluded from encryption.		Files excluded from encryption
	askForConfirmation: Indicates whether confirmation must be requested for the encryption of excluded files.	true, false	N/A
	path: File path. To indicate several files, the "files" list must contain several objects, each with a different "path" property. For example: <pre>"files": [{ "path": "path1" }, { "path": "path2" }]</pre>	String	File path
folders	List of folders to be excluded from encryption.		Folders or masks excluded from encryption
	askForConfirmation: Indicates whether confirmation must be requested for the encryption of excluded folders.	true, false	N/A
	path: Folder path. To indicate several folders, this parameter must be used several times. See the "files" parameter.	String	File path
	recursive: Indicates whether sub-folders are included in the exclusion list.	true, false	Include sub-folders
masks	List of masks to be excluded from encryption.		Folders or masks excluded from encryption
	askForConfirmation: Indicates whether confirmation must be requested for the encryption of excluded files.	true, false	N/A



Parameter	Description	Possible values	SDMC
	path: Path of the mask with the "*.ext" extension to apply the mask. To indicate several masks, this parameter must be used several times. See the "files" parameter.	String	File path
	recursive: Indicates whether sub-folders are included in the exclusion list.	true, false	Include sub-folders

2.5 Stormshield Data Team

! INFORMATION

As of January 2025, Stormshield will no longer offer functional upgrades to the Stormshield Data Team feature. The feature will switch to maintenance mode from this date.

Stormshield Data Team can be configured in the *teamPolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > Team**.

For more information on configuring this feature, see *Configuring Stormshield Data Team* in the Administration guide.



Parameter	Description	Possible values	SDMC
accessToEncryptedFile	Indicates the accessibility of an encrypted file. Allowed values are: <ul style="list-style-type: none">"always" to access it regardless of the certificate status,"notIfRevokedOrCrlExpired" to deny access if the encryption key is revoked or the CRL is not available,"notIfCertificateHasAnIssue" to deny access if the certificate has a warning or error.	always, notIfRevokedOrCrlExpired, notIfCertificateHasAnIssue	Users can access an encrypted file regardless of the status of their certificate, Users cannot access an encrypted file if the certificate of their encryption key is revoked or if the revocation list is not available, Users cannot access an encrypted file if their certificate displays a warning or an error.
allowDecryption	Indicates whether file decryption is allowed.	true, false	Allow encryption
allowDeletion	Indicates whether file deletion is allowed.	true, false	Allow deletion
allowEncryptionAccordingToDefinedRules	Indicates whether encryption is allowed according to the rules defined.	true, false	Allow encryption according to the rules defined
allowSaveAndRestore	Indicates whether backups and restorations are allowed.	true, false	Allow save and restore



Parameter	Description	Possible values	SDMC
closeReportWindow	Indicates when to close the report window. Allowed values are: <ul style="list-style-type: none">"always" for the window to close after encryption,"ifNoWarning" for the window to remain displayed when there is a warning,"never" for the window to remain displayed after encryption.	always, ifNoWarning, never	Closing the report window
excludedFolders	Optional. List of folders to be excluded. This list is recursive.	Character string	N/A
openEncryptedFileInUnsecuredFolder	Defines the behavior when opening an encrypted file in a non-secure folder. Allowed values are: <ul style="list-style-type: none">"allow" to allow it,"deny" to prohibit it,"readonly" to allow it in read-only mode.	allow, deny, readOnly	Opening encrypted files in a non-secured folder
reencryptFilesWhenRemovingCoworkers	Indicates whether files will be encrypted again if a coworker is removed from the rule.	true, false	Encrypt again files when removing coworkers from a rule
secureDragAndDrop	Defines the behavior when files or folders covered by a Data Team rule are copied or moved to a non-secure folder. Allowed values are: <ul style="list-style-type: none">"keepCurrentRule" to apply the rule of the destination folder after moving or copying,"forbidden" to prohibit copying or moving,"noDecryption" to not decrypt the file after moving or copying.	keepCurrent Rule, forbidden, noDecryption	Decrypt when copying or moving, Prohibit copying or moving, Keep encryption when copying or moving
setCreationDateToCurrentDate	Indicates whether the creation date must be the current date.	true, false	Set creation date to current date



Parameter	Description	Possible values	SDMC
setModificationDateToCurrentDate	Indicates whether the modification date must be the current date.	true, false	Set modification date to current date
showCoworkers	Indicates when the rule is displayed. Allowed values are: <ul style="list-style-type: none">"always" so that all users can display the rule,"onlyIfUserIsACoworker" so that only coworkers in the rule can show the rule,	always, onlyIfUserIsACoworker	Show coworkers
showSuccessfullyProcessedFiles	Indicates whether correctly encrypted files are shown in the progress window.	true, false	Show encrypted files in the progress window
updateCoworkerKeyInKnownRules	Indicates whether the coworker's key is updated in the known rules after a key renewal.	true, false	Update a coworker's key in the known rules if the key has been renewed
useLocalCertificateState	Indicates whether the status of the local certificate in the cache must be used if the CRL cannot be downloaded, or if it has expired.	true, false	Use local certificate state in cache if the revocation list cannot be downloaded or if it is expired

2.6 Stormshield Data Disk

Stormshield Data Disk can be configured in the *diskPolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > Disk**.

For more information on configuring this feature, refer to the section *Configuring Stormshield Data Disk* in the Administration guide.

Parameter	Description	Possible values	SDMC
allocationUnitKB	Size of the NTFS clusters used in the virtual disk.	0, 512, 1024 and 4096	N/A



Parameter	Description	Possible values	SDMC
automaticCreation	Optional. Makes it possible to automatically create a volume for a user who connects for the first time.		
	autoMount: Enables or disables the automatic mounting of the volume every time the user connects.	true, false	Mount the volume automatically when the user connects to SDS
	mountLetter: Letter used for the mounted disk. If the letter is not available, the first letter available in reverse alphabetical order will be taken (starting with Z).	letter between D and Z	Drive letter
	showFinalReport: Enables or disables the display of a final report.	true, false	Display a report after the creation
	sizeMB: Optional. Size in MB to allocate to the volume to be created. If no value is entered, the size will amount to 10% of the available size on the client workstation.	Positive integer.	Volume size
	vboxFullPath: Name and location of the special encrypted .vbox file on which the volume relies.	Path	Full path to the .vbox file associated with the volume
enableCompression	Indicates whether compression of the volume is allowed.	true, false	N/A
enableQuickCreation	Indicates whether quick creation is allowed.	true, false	Allow quick creation of Disk volume
enableQuickFormat	Indicates whether quick format is allowed.	true, false	Allow quick format of Disk volume
enableRescueFileModification	Indicates whether modification of vboxsave backup files is allowed.	true, false	N/A
enableExpertMode	Indicates whether modification of vboxsave backup files is allowed in the associated vbox directory.	true, false	N/A
fileSystem	File system used for mounted volumes.	NTFS, FAT32, FAT	File system
maxSizeMB	Maximum size allowed for the creation of a volume in MB.	Positive integer.	Maximum size allowed



Parameter	Description	Possible values	SDMC
mountAsNonRemovable	Indicates whether the mounted disk will be removable.	true, false	Mount volumes as non removable disks
volumeName	Name given to created volumes. By default "SDSDiskVolume".	String	Volume name
encryptionAlgorithm	Indicates the encryption mode used for the volume. Allowed values are: <ul style="list-style-type: none">"AES-256" for the AES CBC encryption mode (default value),"AES-XTS-256" for the AES-XTS encryption mode offering a better data protection and recommended by the ANSSI.	[AES-256], AES-XTS-256	N/A

2.7 Stormshield Data Mail

Stormshield Data Mail can be configured in the *mailPolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > Mail**.

For more information on configuring this feature, refer to the section *Configuring Stormshield Data Mail* in the Administration guide.

Parameter	Description	Possible values	SDMC
enableSMime	Indicates whether messages encrypted with S/MIME can be sent and received. Currently, this parameter has no effect and will be operational in a future version.	true, false	N/A
enablePGP	Indicates whether messages encrypted with PGP can be sent and received.	true, false	Allow PGP messages encryption/decryption
encryptByDefault	Indicates whether encryption must be automatically enabled when new messages are being composed.	true, false	Enable messages encryption by default



Parameter	Description	Possible values	SDMC
signByDefault	Indicates whether signing must be automatically enabled when new messages are being composed.	true, false	Enable messages signature by default
signatureType	Type of signature to use when composing signed messages.	clear, opaque	Type of signature to sign messages (S/MIME only)
updateAddressBookWithSignedMailCertificates	Indicates whether the signature certificate associated with the e-mail address is imported into the user's trusted address book, and whether it is imported automatically or manually by the user.		
	automatic Allowed values are: <ul style="list-style-type: none"> "trustedAuthorities" to import certificates with a trusted issuer, "no" to not import certificates. 	trusted Authorities, no	Allow automatic updates of the trusted address book: <ul style="list-style-type: none"> Only for known authorities No
	manual Allowed values are: <ul style="list-style-type: none"> "anyAuthority" to allow the import of certificates from any source, "trustedAuthorities" to import certificates with a trusted issuer, "no" to not import certificates. 	anyAuthority, trustedAuthorities, no	Allow manual update of the trusted address book: <ul style="list-style-type: none"> For all authorities, Only for known authorities, No
keepSignatureOnSecurityDeletion	Indicates whether the signature of a message must be kept when its protection is lifted.	true, false	N/A
showOperationInProgressDialog	Indicates whether a loading window must be shown whenever an operation lasts longer than three seconds.	true, false	N/A
sensitivityLabelsBehaviour	Optional. When a user sends a message with a Microsoft Purview Information Protection sensitivity label, SDS Enterprise checks the presence of the label in this list and the security action associated with the label.		Automatic encryption and signature with Microsoft Purview



Parameter	Description	Possible values	SDMC
	labelID: name of the label as set in the Microsoft Purview Information Protection administration console.	string	
	behavior: minimum security configuration to be applied to the message.	sign, encrypt, signAndEncrypt	

2.8 Stormshield Data Sign

Stormshield Data Sign can be configured in the *signPolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > Sign**.

For more information on configuring this feature, see *Configuring Stormshield Data Sign* in the Administration guide.

Parameter	Description	Possible values	SDMC
allowCoSigning	Indicates whether the user is allowed to co-sign files.	true, false	Allow file co-signature
allowCounterSigning	Indicates whether the user is allowed to counter-sign files.	true, false	Allow file counter-signature
allowOverSigning	Indicates whether the user is allowed to over-sign files.	true, false	Allow file over-signature
allowSigning	Indicates whether the user is allowed to sign files.	true, false	Allow file signature
allowSigningOnActiveContent	Indicates whether the user is allowed to sign files containing active content.	true, false	Allow file signature when active content is detected
defaultSignExtension	Default file extension for signed files.	".p7f", ".p7m"	Default file extension
displayDocumentBeforeSigning	Indicates whether the user must view a file before signing it.	true, false	Always show file before signing
informUserAboutActiveContentInWordFiles	Indicates whether the user must be informed that a Word file contains active content before being able to sign it. This parameter applies only to files in Microsoft Word version 2000 and higher.	true, false	Inform user when active content is detected in the Microsoft Word file before signing
informUserAboutMacrosInPdfFiles	Indicates whether the user must be informed that a PDF file contains macros before being able to sign it.	true, false	Inform user when macros are detected in the PDF file before signing



Parameter	Description	Possible values	SDMC
informUserAboutMacro sInWordFiles	Indicates whether the user must be informed that a Word file contains macros before being able to sign it. This parameter applies only to files in Microsoft Word versions 97 to 2003.	true, false	Inform user when macros are detected in the Microsoft Word file before signing
preselectMailToAskFor Signature	When the document signing process is complete, the user can request the preparation of an e-mail addressed to coworkers in order to inform them that the document has been signed. If the document was previously signed, the recipients list is pre-filled with the co-signers' email addresses; This option relates to the check box in the signature wizard.	true, false	N/A
preselectMailToNotifyC oWorkers	When the document signature process is over, the user may request the preparation of an e-mail addressed to coworkers in order to ask them to sign the document. This option relates to the check box in the signature wizard.	true, false	N/A

2.9 Stormshield Data Shredder

Stormshield Data Shredder can be configured in the *shredderPolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > Shredder**.

For more information on configuring this feature, refer to the section *Configuring Stormshield Data Shredder* in the Administration guide.

Parameter	Description	Possible values	SDMC
addDesktopIcon	Indicates whether a Stormshield Data Shredder shortcut will be added to the Windows desktop to enable dragging and dropping.	true, false	Add desktop shortcut
allowBinShredding	Indicates whether the user is allowed to shred files in the bin.	true, false	N/A
allowDragAndDropOnShredderIcon	Indicates whether the user is allowed to shred files by dragging and dropping on the Shredder icon.	true, false	Enable dragging and dropping items on the SD Shredder icon
allowFileShredding	Indicates whether the user is allowed to shred files.	true, false	Allow file shredding



Parameter	Description	Possible values	SDMC
allowFolderShredding	Indicates whether the user is allowed to shred folders.	true, false	Allow folder shredding
allowShreddingInterruption	Indicates whether the user is allowed to interrupt shredding operations.	true, false	Allow the interruption of shredding operations
confirmForEachFile	If several files are being shredded, indicates whether user confirmation is required for each file.	true, false	Confirm for each file Confirm only once for all files
exclusionList	Specifies the parameters of the exclusion list. To use this list, refer to exclusionList section .		N/A
readOnlyFilesShredding	Indicates how to process read-only files. Allowed values are: <ul style="list-style-type: none">"neitherShredNorNotify" to neither shred the file nor notify the user,"doNotShredButNotify" to not shred the file but notify the user,"askConfirmation" to request confirmation before shredding,"treatAsUsual" to shred according to the same rules applied to other files.	neitherShred NorNotify, doNotShred ButNotify, askConfirmation, treatAsUsual	Never shred Report files Ask confirmation Process like standard files
shredHiddenFiles	Indicates whether the user is allowed to shred hidden files.	true, false	N/A
shreddingPatternBytes	Bits used to replace the content of shredded files	List of positive integers between 0 and 255	N/A

2.9.1 exclusionList section

Using an exclusion list, you can exclude some files to prevent them from being shredded by mistake. The following parameters are specified in the *shredderPolicy.exclusionList* section of the *.json* file. This list is optional.

Parameter	Description	Possible values	SDMC
displayWarning	Indicates whether a warning window must be displayed if an operation could not be completed because of the exclusion list.	true, false	N/A



Parameter	Description	Possible values	SDMC
files	Optional. List of files to be excluded from shredding.		N/A
	askForConfirmation: Indicates whether confirmation must be requested for the shredding of excluded files.	true, false	N/A
	path: File path. To indicate several files, the "files" list must contain several objects, each with a different "path" property. For example: <pre>"files": [{ "path": "path1" }, { "path": "path2" }]</pre>	String	N/A
folders	Optional. List of folders to be excluded from shredding.		N/A
	askForConfirmation: Indicates whether confirmation must be requested for the shredding of excluded folders.	true, false	N/A
	path: Folder path. To indicate several folders, this parameter must be used several times. See the "files" parameter.	String	N/A
	recursive: Indicates whether sub-folders are included in the exclusion list.	true, false	N/A
masks	Optional. List of masks to be excluded from shredding.		N/A
	askForConfirmation: Indicates whether confirmation must be requested for the shredding of excluded files.	true, false	N/A
	path: Path of the mask with the "*.ext" extension to apply the mask. To indicate several masks, this parameter must be used several times. See the "files" parameter.	String	N/A
	recursive: Indicates whether sub-folders are included in the exclusion list.	true, false	N/A

2.9.2 shreddingList section

Files included in shredding lists are automatically shredded at a predetermined time or when a predetermined event takes place. The following parameters are specified in the *shredderPolicy.shreddingList* section of the *.json* file.



Parameter	Description	Possible values	SDMC
askConfirmation	Indicates whether a confirmation is required before automatic shredding.	true, false	N/A
displayReport	Indicates whether to display a report after automatic shredding.	true, false	N/A
files	Optional. List of files to shred automatically.		N/A
	path: File path. To indicate several files, the "files" list must contain several objects, each with a different "path" property. For example: <pre>"files": [{ "path": "path1" }, { "path": "path2" }]</pre>	String	N/A
fixedTimesInSeconds	List of times at which files are automatically shredded. Expressed in number of seconds from 00:00. For example, 1:30 a.m. is represented by a value of 5400.	List of positive whole integers	N/A
folders	Optional. List of folders to shred automatically		N/A
	path: Folder path. To indicate several folders, this parameter must be used several times. See the "files" parameter.	String	N/A
	recursive: Indicates whether sub-folders are included in the shredding list.	true, false	N/A
intervalMinutes	Optional. Frequency with which files are automatically shredded. Expressed in minutes.	Positive integer.	N/A
masks	Optional. List of masks to shred automatically.		N/A
	path: Path of the mask with the "*.ext" extension to apply the mask. To indicate several masks, this parameter must be used several times. See the "files" parameter.	String	N/A
	recursive: Indicates whether sub-folders are included in the shredding list.	true, false	N/A




Parameter	Description	Possible values	SDMC
onDisconnection	Enables automatic shedding when disconnecting from SDS Enterprise	true, false	N/A
onScreenSaverStarted	Enables automatic shredding when screensaver starts.	true, false	N/A
onSessionLock	Enables automatic shredding when locking SDS Enterprise session.	true, false	N/A

2.10 Stormshield Data Share

Stormshield Data Share can be configured in the *sharePolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > Share**.

For more information on configuring this feature, refer to the section *Configuring Stormshield Data Share* in the Administration guide.

Parameter	Description	Possible values	SDMC
<ul style="list-style-type: none">dropboxPolicyoodrivePolicyoneDrivePolicyoneDriveForBusinessPolicysharepointPolicy	Indicates how SDS Enterprise must protect Dropbox, Oodrive, OneDrive, OneDrive for Business and SharePoint shared spaces. Each of these parameters is a separate object whose individual properties are detailed in the following lines.		<ul style="list-style-type: none">DropboxOneDriveOneDrive for BusinessSharePointOoDrive
	protect: Indicates whether the synchronized space must be automatically protected.	true, false	Enable/Disable the button 
	subfoldersToProtect: Specifies the list of sub-folders to be protected in the shared space. Applies only if "protect" : true. An empty list means that the entire shared space is protected. Examples: <ul style="list-style-type: none">["Documents"]["Folder1", "Folder2\\SubFolder"]	List of strings	Advanced



Parameter	Description	Possible values	SDMC
ruleCreation	<p>Optional. When creating an automatic folder protection rule, allows you to force the creation of a shared or local rule or to leave the choice to the user. The possible values are:</p> <ul style="list-style-type: none"> • "forceSharedRule" to always create protection rules as shared rules. • "forceLocalRule" to always create protection rules as local rules. • "userChoice" to allow the user to choose whether or not to share the rule. 	<p>forceSharedRule,</p> <p>forceLocalRule,</p> <p>userChoice</p>	<p>Always create protection rules as shared rules</p> <p>Always create protection rules as not shared rules</p> <p>Allow choosing the type of protection rules during creation</p>

2.11 Directories

The directories to be used to provide user certificates are defined in the *directories* section of the *.json* file, which is divided into several sub-sections: *ldap* and *pgp*.

For more information on configuring this feature, refer to the section *Configuring corporate directories* in the Administration guide.

2.11.1 ldap section

LDAP directories are configured in the *ldap* section described in the table below. In the SDMC administration console, the equivalent parameters are found in **Policies > Directories > LDAP**.

Parameter	Description	Possible values	SDMC
addWildcardSuffixInFilter	Specifies whether to automatically suffix search criteria with "*". This is transparent to the user.	true, false	Suffix search criteria by "*"
addWildcardPrefixInFilter	Specifies whether to automatically prefix search criteria with "*". This is transparent to the user.	true, false	Prefix search criteria by "*"
addUserCertificateBinaryFilter	Indicates whether "usercertificate;binary=*" must be added to the search filter to return only LDAP entities that have a certificate.	true, false	N/A
ldapAddressBookList	List of unique IDs in LDAP directories accessible to users. You will find the IDs in the list of LDAP directories in the ldapData section of the <i>.json</i> file.	List of unique character strings.	Add from library
automaticUpdate	Optional. Indicates how to manage updates of the trusted address book and its certificates. Automatic updates are applied only if all parameters are fulfilled.		Update the directory automatically



Parameter	Description	Possible values	SDMC
	downloadCrlsUponVerification: Indicates whether the CRL must be downloaded when verifying the certificate.	true, false	N/A
	onPeriodicHours: Frequency with which updates are performed (in hours).	Positive integer between 1 and 24	Update frequency
	onUserConnection: indicates whether the update begins when the user logs in.	true, false	Start the directory update when the user connects to the SDS account
	updateValidCertificatesWithNewerOnes: Indicates whether valid certificates must be updated with more recent certificates.	true, false	Update certificates saved in the trusted directory with most recent certificates from an LDAP directory
	updateOnlyFromCAs: Optional. List of unique IDs of authorities from which updates are to be applied. You will find the IDs in the list of authorities in the certificateData section of the <i>.json</i> file. If this field is empty, all authorities will be taken into account.	List of character strings, each of which corresponds to the "id" field of an object in the "certificateData" list of the policy.	N/A
	expiredCertificates: Indicates how to manage the deletion of expired certificates.		Deletion of expired certificates
	updateWithNewerOnes: Indicates whether they must be updated with more recent certificates. This criterion is based on the list provided by the parameter "updateOnlyFromCAs".	true, false	Update expired certificates
	removeFromLocalDirectory: Indicates whether the certificate must be removed from the local directory.	true, false	Delete automatically



Parameter	Description	Possible values	SDMC
	removeOnlyFromCAs: Optional. List of unique IDs of authorities from which deletion will be applied. You will find the IDs in the list of authorities in the certificateData section of the <i>.json</i> file. If this field is empty, all authorities will be taken into account.	List of character strings, each of which corresponds to the "id" field of an object in the "certificateData" list of the policy.	Selection of CAs that issue certificates to be deleted automatically when they expire
	revokedCertificates: Indicates how to manage the deletion of expired certificates.		Deletion of certificates revoked
	updateWithNewerOnes: Indicates whether they must be updated with more recent certificates. This criterion is based on the list provided by the parameter "updateOnlyFromCAs".	true, false	Update revoked certificates
	removeFromLocalDirectory: Indicates whether the certificate must be removed from the local directory.	true, false	Delete automatically
	removeOnlyFromCAs: Optional. List of unique IDs of authorities from which deletion will be applied. You will find the IDs in the list of authorities in the certificateData section of the <i>.json</i> file. If this field is empty, all authorities will be taken into account.	List of character strings, each of which corresponds to the "id" field of an object in the "certificateData" list of the policy.	Selection of CAs issuing certificates to delete automatically when they are revoked
	missingCertificates: Indicates how to handle the deletion of missing certificates. The parameters are the same as those for "expiredCertificates" (see above).		Deletion of certificates removed from the LDAP directory
	updateWithNewerOnes: Indicates whether they must be updated with more recent certificates. This criterion is based on the list provided by the parameter "updateOnlyFromCAs".	true, false	Update missing certificates when searching for coworkers
	removeFromLocalDirectory: Indicates whether the certificate must be removed from the local directory.	true, false	Delete automatically



Parameter	Description	Possible values	SDMC
	removeOnlyFromCAs: Optional. List of unique IDs of authorities from which deletion will be applied. You will find the IDs in the list of authorities in the certificateData section of the <i>.json</i> file. If this field is empty, all authorities will be taken into account.	List of strings	Selection of CAs issuing certificates to delete automatically when they are removed from the LDAP directory

2.11.2 pgp section

The following parameters are specified in the *directories.pgp* section of the *.json* file. In the SDMC administration console, the equivalent parameters are found in **Policies > Directories > PGP**.

Parameter	Description		SDMC
wkdServers	Parametric URLs to servers hosting public keys that can be accessed by the WKD (Web Key Directory) schema. They must be in the following form, the sections in bold being kept as is: <ul style="list-style-type: none"> WKD "advanced": <a href="https://openpgpkey.optional-sub-domains.domain.toplevel/.well-known/openpgpkey/<d>/hu/<k>?get_parameters=optional">https://openpgpkey.optional-sub-domains.domain.toplevel/.well-known/openpgpkey/<d>/hu/<k>?get_parameters=optional WKD "direct": <a href="https://optional-sub-domains.domain.toplevel/.well-known/openpgpkey/hu/<k>?get_parameters=optional">https://optional-sub-domains.domain.toplevel/.well-known/openpgpkey/hu/<k>?get_parameters=optional 	List of strings	WKD servers

2.12 Certificate revocation

Revocation can be configured in the *revocationPolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Authorities**.

For more information on how to configure the feature, refer to the section *Configuring certificate revocation control* in the Administration guide.

Parameter	Type Description	Prescribed values	SDMC
checkCertificateRevocation	Optional. Indicates whether certificate revocation must be verified.	true, false	N/A
displayWarningDBCORRUPTED	Shows a warning message when the local CRL database is corrupted.	true, false	N/A



Parameter	Type Description	Prescribed values	SDMC
displayWarningDBDeleted	Shows a warning message when the local CRL database has been erased.	true, false	N/A
fileTimeOutInSeconds	Maximum time in seconds allocated to downloading the CRL from a file.	Positive integer.	N/A
httpTimeOutInSeconds	Maximum time in seconds allocated to downloading the CRL from an HTTP link.	Positive integer.	N/A
issuers	List of authority certificates and recovery certificates to be used in your policies.		
	certificateID: Unique ID of the certificate in the policy. You will find the identifier in the list of certificates in the certificateData section of the <i>.json</i> file.	Unique character string	
	crlDownloadFrequency: Frequency with which the CRL is downloaded. Allowed values are: <ul style="list-style-type: none"> • "onFirstCryptoOperation" (default value) the first time an encryption or decryption operation is conducted, • "WhenExpired" when the certificate expires, • "always" every time a certificate is used, • "never" never download the CRL. 	OnFirst Crypto Operation, WhenExpired, Always, Never	N/A
	methods: List of CRL download methods.		Add from library
	type: Type of revocation method.	"CRL" "OCSP"	N/A
	url: URL used for the download.	String	N/A
ldapTimeOutInSeconds	Maximum time in seconds allocated to downloading the CRL from a LDAP link in seconds.	Positive integer.	N/A
validityDurationInDays	CRL validity in days.	Positive integer. [max 365]	Validity period of revocation lists

2.13 Distribution points

Policy distribution points can be configured in the *distributionPointPolicy* section of the *.json* file. The table below describes their parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Distribution**.

For further information, refer to the section *Configuring policy distribution points* in the Administration guide.



Parameter	Description	Prescribed values	SDMC
urls	List of URLs indicating the full path(s) to the .jwt policy file of your choice. SDS Enterprise checks the list of distribution points in the order you have set. It will apply the first valid policy that it detects. URLs must have an http://, https://, or file:// prefix and must be separated by commas. For example: "http://test.com/file.jwt", "file://10.1.1.1/file.jwt"	List of URLs	Full path to the policy file



3. Configuring advanced parameters in the registry base

Some advanced parameters in SDS Enterprise must be configured in the Windows registry base.

To edit the registry base:

1. Access the registry by running **regedit.exe** with administrator rights.
2. In the tree view, select the key shown or create it if necessary.
3. Change the value of the key.
4. Quit the registry database.
5. Restart the machine.

3.1 Team Feature

3.1.1 Changing the dates of the last access

When Stormshield Data Team is installed on a workstation, the date of the last access changes when a folder is browsed. The `AccessTimeAction` registry key restores the true date of last access to the files.

Key	<code>AccessTimeAction</code> (DWORD)
Location	<code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SBoxTeamDrv\Parameters</code>
Values	<ul style="list-style-type: none">• <code>0x00000000</code>: The access date modified by Stormshield Data Team is kept (default value),• <code>0x00000001</code>: The access date is restored on standard file systems,• <code>0x00000002</code>: The access date is restored on NFS file systems,• <code>0x00000008</code>: The access date is restored on standard file systems with a potential slowdown in performance. This option enables compatibility with file systems considered standard, such as NAS EMC or non-standard CIFS servers. <p>In general, the default value <code>0x00000000</code> is recommended. However, when using an archive solution based on a NAS EMC, the value <code>0x00000008</code> is recommended.</p>

3.1.2 Check user key certificate

The user's encryption key certificate is checked every two hours [120 minutes].

You can modify this value, which is taken into account when the user logs in, by creating the following registry key:

Key	<code>CheckCertificateTimeout</code> (REG_SZ)
Location	<code>HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\Team\</code> or <code>HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Suite\Team\</code>
Value	<ul style="list-style-type: none">• Positive integer.



3.2 Manage encryption and signature keys

For the three registry keys below, the location differs according to the type of account:

KS1: Password account with a single key to sign and/or encrypt.

KS2: Password account with two different keys to sign and encrypt.

GP1: Card account with a single key to sign and/or encrypt.

GP2: Card account with two different keys to sign and encrypt.

3.2.1 Specify that keys are generated by SDS Enterprise

In card or token mode (GP1 or GP2), encryption and signature keys are generated by the card/token, i.e. by the card itself or in memory, depending on the manufacturer's implementation or configuration of its PKCS#11 layer.

You can specify that keys are generated exclusively by SDS Enterprise in memory. This allows the keys to be exported later.

Create the following registry key:

Key	InternalKeys (REG_SZ)
Locations	Suite\SBBox.KeyRenewalWizardGP\ or HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP\ HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP1\ or HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP1\ HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP2\ or HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP2\ or HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP2\
Value	<ul style="list-style-type: none">0

3.2.2 Choose how to keep keys for exporting later

If an encryption or signature key has been generated by SDS Enterprise in memory (if `InternalKeys = 0`), it will be exportable. For this, you must assign the value 1 to the `ExportKeys` registry key in order to display the window offering the user two choices:

- Save this key in a PKCS#12 file and assign a password,
- Copy this key to the user's account file.

Create the following registry key:

Key	ExportKeys (REG_SZ)
Location	HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP\ or HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP\ HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP1\ or HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP1\ HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP2\ or HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP2\ or HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\SBBox.KeyRenewalWizardGP2\
Value	<ul style="list-style-type: none">1



3.3 Moving folders available offline

The *cachemov.exe* utility can be used to move the - <%WINDIR%>\CSC - system folder, which contains files available offline.

Stormshield Data Team must be configured as follows to manage this particular environment:

Key	SkipFolderR (DWORD)
Location	HKLM\SYSTEM\CURRENTCONTROLSET\Services\SBoxTeamDrv\Parameters
Value	Add the folder containing the CSC database.

3.4 Keeping performance optimal on the workstation

When Stormshield Data Team is used, users' workstations may slow down. To keep the usual levels of performance, the following registry keys can be applied:

3.4.1 Improving performance when browsing encrypted trees

To reduce the time it takes to determine whether a folder is encrypted in "smart card" mode (this determines the icon of the folder), the value of the *OverlayIconAccuracy* parameter can be changed.

Key	OverlayIconAccuracy (DWORD)
Location	HKEY_LOCAL_MACHINE\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Team
Value	<ul style="list-style-type: none">0x40: Greatly reduces the time it takes to determine whether a folder is encrypted in smart card or token mode.

3.4.2 Excluding Windows processes that access encrypted folders

Some Windows processes can slow down the workstation by regularly accessing folders that Stormshield Data Team encrypts.

To reduce the frequency of these slowdowns, you can exclude in the registry database the processes that are considered safe and do not cause any file modifications. If the *SkipApp* key does not exist, you can create it by choosing a REG_MULTI_SZ value.

Key	SkipApp (MULTI_SZ)
Location	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SboxTeamDrv\Parameters



Value	Add one process to exclude per line. We recommend that you exclude the following processes: SearchIndexer.exe searchUI.exe MsMpEng.exe SearchProtocolHost.exe SearchFilterHost.exe mobsync.exe msdtc.exe mstsc.exe mobsync.exe wfica32.exe vmtoolsd.exe SecurityHealthService.exe SearchApp.exe NisSrv.exe As well as the specific Dell processes: HostStorageService.exe HostControlService.exe
-------	---

3.4.3 Excluding Windows Defender extensions and scans

To prevent your workstation from slowing down, you can also exclude the extensions and scans that Windows Defender runs:

Key	Extensions (DWORD)
Location	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions
Value	Add the list of extensions to exclude. We recommend excluding the following extensions: .box, .sbox, .sbt, .sdsx, .usi, .usr.
Key	Processes (DWORD)
Location	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions
Value	Add the list of processes to exclude. We recommend that you exclude the following processes: <i>SBDSRV</i> , <i>SBoxDiskSrv</i> as well as antivirus and other EDR processes.

3.5 Disabling automatic suggestion of coworkers

When selecting the coworkers you want to share the folder with, coworkers who hold the Windows permissions that enable accessing the folder concerned are automatically suggested in a group which name is **Windows permissions**.

You can disable this feature by creating the following registry key:

Key	SuggestCoworkersThroughACL (DWORD)
Location	HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Kernel\
Value	• 0

3.6 Configure the filter for the coworker search in the LDAP directory



When selecting coworkers authorized to access a secure folder, the LDAP directory search is based on the common name by default.

If the common name is not enough, you can configure a custom search filter to search through multiple LDAP attributes, using the following registry keys:

Key	SearchFilter (REG_SZ)
Location	HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Properties\CoworkerSelector
Value	<p>Specify the filter you want to apply when performing an LDAP search. Use the logical connectors "&" [and] and " " [or]. For example:</p> <ul style="list-style-type: none"> ((cn=?) (mail=?)) searches for the character string entered by the user in the common name OR in the email address. (&((cn=?) (mail=?)) (usercertificate;binary=*)) searches for the string entered by the user in the common name OR in the email address AND the user must have a certificate in the LDAP directory. <p>The "?" character is replaced by the character string entered by the user in the search field.</p>
Key	SearchPattern (REG_SZ)
Location	HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Properties\CoworkerSelector
Value	Optional key. Replaces the default character "?" used in the filter if necessary.

3.7 Show license key value

In the **About SDS Enterprise** window, the license key value is hidden.

You can display the value of the key by creating the following registry key:

Key	DontShowLicenceKey (REG_SZ)
Location	HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\Logon\ or HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Suite\Logon\
Value	<ul style="list-style-type: none"> 0

3.8 Manage card or token readers

3.8.1 Specify a card or token reader

If several card or token readers are connected to the workstation (e.g. a standard reader and a 3G network card), all readers are taken into account.

You can select a specific reader by defining a filter to identify it. In this case, only the drive indicated by the `SlotInfoDescriptionPrefix` or `SlotInfoManufacturerIdPrefix` registry keys is taken into account by SDS Enterprise.

Create the following registry key:

Key	SlotFilterOn (REG_SZ)
-----	-----------------------



Location	HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\Logon\ or HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Suite\Logon\
Value	<ul style="list-style-type: none">• 1

3.8.2 Filter card or token readers by their description

If several card or token readers are connected to the workstation (e.g. a standard reader and a 3G network card), all readers are taken into account.

You can specify a prefix to filter on the description field returned by the reader (*slotinfo.SlotDescription* at PKCS#11 level). For example, if you specify the SER prefix, SERIAL will be accepted, whereas USB will not.

Create the following registry key:

Key	SlotInfoDescriptionPrefix (REG_SZ)
Location	HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\SlotFilter\ or HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Suite\SlotFilter\
Value	<ul style="list-style-type: none">• Case-sensitive string

3.8.3 Filter card or token readers by manufacturer ID

If several card or token readers are connected to the workstation (e.g. a standard reader and a 3G network card), all readers are taken into account.

You can specify a prefix to filter on the *ManufacturerId* field returned by the reader (*slotinfo.ManufacturerId* at PKCS#11 level). For example, if you specify the AX prefix, AXALTO will be accepted, while GEMPLUS will not.

Create the following registry key:

Key	SlotInfoManufacturerIdPrefix (REG_SZ)
Location	HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\SlotFilter\ or HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Suite\SlotFilter\
Value	<ul style="list-style-type: none">• Case-sensitive string

3.8.4 Prohibit modification of card or token type

By default, the user is authorized to modify the type of card or token defined in the **card extension configurator**.

You can prohibit user modification by creating the following registry key:

Key	CPLCanChangePKCS11 (REG_SZ)
Location	HKEY_CURRENT_USER\SOFTWARE\Arkoon\Security BOX Suite\External PKCS11 Policy\ or HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Suite\External PKCS11 Policy\
Value	<ul style="list-style-type: none">• 0

3.9 Replace default icon for Share-protected collaborative folders



By default, synchronized workspace folders protected by an automatic Share protection rule do not have an icon to identify them.

You can replace the default Windows folder icon with a custom SDS Enterprise icon for easy identification.

To replace the Windows folder icon, create the following registry key:

Key	cloudSecuredFolderIcon
Location	HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Share
Value	<ul style="list-style-type: none">• 0: feature disabled. Folders protected by an automatic protection rule have the default Windows folder icon. Same behavior as when the key is missing.• 1: the default Windows folder icon is replaced by the custom SDS Enterprise icon when the folder is protected by an automatic protection rule.

The custom icon is displayed only on folders with the automatic protection rule, not on sub-folders. Files in folders have a small blue padlock.

This feature does not apply to local folders protected by automatic protection rules.



4. Further reading

Additional information and answers to questions you may have are available in the [Stormshield knowledge base](#) (authentication required).



STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2025. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.